Safety control with performance guarantees of cooperative systems using compositional abstractions

Pierre-Jean Meyer, Antoine Girard, Emmanuel Witrant

Safety control with performance guarantees of cooperative systems using compositional abstractions ⋆

Pierre-Jean Meyer [*,**] **Antoine Girard** [*] **Emmanuel Witrant** [**]

[*] *Univ. Grenoble Alpes, CNRS, LJK, F-38000 Grenoble, France*
{Pierre-Jean.Meyer ; Antoine.Girard}@imag.fr
[**] *Univ. Grenoble Alpes, CNRS, GIPSA-lab, F-38000 Grenoble, France*
Emmanuel.Witrant@ujf-grenoble.fr

Abstract: In this paper, the monotonicity property is exploited to obtain symbolic abstractions, in the sense of alternating simulation, of a class of nonlinear control systems subject to disturbances. Both a centralized and a compositional approaches are presented to obtain such abstractions, from which controllers are synthesized to satisfy safety specifications and optimize a performance criterion using a receding horizon approach. Performance guarantees on the trajectories of the controlled system can be obtained with both approaches. The controller synthesis and performance guarantees are illustrated and compared on the temperature regulation in a building.

Keywords: Symbolic control; Compositional synthesis; Monotone systems.

1. INTRODUCTION

The problem of control synthesis for complex dynamical systems has been approached by various methods, such as robust $\mathcal{H}_\infty$ control (Skogestad and Postlethwaite, 2005) or model predictive control (Rawlings and Mayne, 2009). The method considered in this paper consists in creating an abstraction of the model with some behavioral relationship ensuring that the control applied to the abstraction also controls the original model. These abstractions can be obtained in several ways, using a bisimulation algorithm (Alur et al., 2000), computing reachable sets (Reißig, 2009) or by state quantization (Pola et al., 2008). All these approaches provide an abstraction where the states are *symbols* representing sets of states in the original model, with the number of symbols acting as a trade-off between the precision on the state information and the simplicity of the abstraction model.

The abstraction model may differ depending on the control objectives, the desired simplifications on the original model, the available information and to what extend we can ignore part of this information. When the abstraction is a finite model, as it is the case in this paper, we can enforce safety specifications by using a fixed point algorithm and optimize a performance criterion using a receding horizon controller (Ding et al., 2014) similarly to a model predictive control strategy (Rawlings and Mayne, 2009). The advantage of the abstraction in this case is that all the computations can be done offline and the resulting control implementation thus only corresponds to a look-up table. To overcome the exponential complexity of creating such a finite model, we propose a compositional approach taking an additional tradeoff between precision and simplicity of the abstraction by decomposing the system into subsystems with partial information on the state. Similarly to an assume-guarantee reasoning (Alur and Henzinger, 1999), the controller synthesis for each subsystem assumes that the safety specifications are met for the others.

We consider a class of monotone nonlinear systems (more precisely, cooperative systems), implying that their trajectories preserve some partial order on the state (e.g. see Smith (1995) for autonomous systems and Angeli and Sontag (2003) for controlled systems). This monotonicity property significantly facilitates creating an abstraction and proving the required behavioral relationship. For example in Moor and Raisch (2002), over-approximations of reachable sets are directly obtained using the monotonicity. This method can be extended to a class of non-monotone systems satisfying the mixed-monotonicity property, where the dynamics are decomposed into increasing and decreasing components (Coogan and Arcak, 2015). Monotone systems appear in numerous fields, such as molecular biology (Sontag, 2007), chemical networks (Belgacem and Gouzé, 2013) or thermal dynamics in buildings, which is the application considered in this paper.

The structure of this paper is as follows. The class of systems considered and some preliminary definitions are presented in Section 2, followed by the problem formulation in Section 3. In Section 4 we present a centralized method to synthesize a controller based on a symbolic abstraction of the system. A compositional approach is then given in Section 5 where the previous method is used on subsystems with a partially observable state. For both methods, we provide performance guarantees on the controlled trajectories of the original system. Finally, in Section 6, our methodological results are illustrated and compared on the temperature control in a building.

⋆ This work was partly supported by a PhD scholarship and the research project COHYBA funded by Région Rhône-Alpes.

2. PRELIMINARIES

2.1 Cooperative systems

We consider a class of nonlinear systems given by:

$$\dot{x} = f(x, u, w), \tag{1}$$

where $x \in \mathbb{R}^n$, $u \in [\underline{u}, \overline{u}] \subseteq \mathbb{R}^p$ and $w \in [\underline{w}, \overline{w}] \subseteq \mathbb{R}^q$ denote the state, the control input and the disturbance input, respectively. The trajectories of (1) are denoted $\Phi(\cdot, x_0, \mathbf{u}, \mathbf{w})$ where $\Phi(t, x_0, \mathbf{u}, \mathbf{w})$ is the state reached at time $t \in \mathbb{R}_0^+$ from initial state $x_0 \in \mathbb{R}^n$, under piecewise continuous control and disturbance inputs $\mathbf{u} : \mathbb{R}_0^+ \to [\underline{u}, \overline{u}]$ and $\mathbf{w} : \mathbb{R}_0^+ \to [\underline{w}, \overline{w}]$, respectively.

Let $\geq$ and $>$ denote the componentwise inequalities on the appropriate space $\mathbb{R}^m$, $m \in \{n, p, q\}$. We also extend the definition of these inequalities to functions of time $\mathbf{z}, \mathbf{z}' : \mathbb{R}_0^+ \to \mathbb{R}^m$ with $\mathbf{z} \geq \mathbf{z}' \Leftrightarrow \forall t \geq 0,\ \mathbf{z}(t) \geq \mathbf{z}'(t)$. In Angeli and Sontag (2003), a dynamical system with inputs is said to be monotone when its trajectories preserve a partial ordering on the states. In this paper, we focus on cooperative systems where the partial orderings are $\geq$.

Definition 1. (Cooperative system). System (1) is cooperative if for all $x \geq x'$, $\mathbf{u} \geq \mathbf{u}'$, $\mathbf{w} \geq \mathbf{w}'$ it holds for all $t \geq 0$, $\Phi(t, x, \mathbf{u}, \mathbf{w}) \geq \Phi(t, x', \mathbf{u}', \mathbf{w}')$.

Definition 1 is assumed to be satisfied for all the results of this paper. Characterization of such systems based on the vector field f can be found in Angeli and Sontag (2003).

2.2 Alternating simulation

In Tabuada (2009), a system is defined as a quadruple $S = (X, X_0, U, \longrightarrow)$ consisting of: a set of states X; a set of initial states $X_0 \subseteq X$; a set of inputs U; a transition relation $\longrightarrow \subseteq X \times U \times X$. A transition $(x, u, x') \in \longrightarrow$ is equivalently written $x \xrightarrow{u} x'$ or $x' \in Post(x, u)$. $U(x)$ denotes the set of inputs u such that $Post(x, u) \neq \emptyset$. A trajectory of S is an infinite sequence $(x^0, u^0, x^1, u^1, \dots)$ such that $x^0 \in X_0$ and for all $i \in \mathbb{N}$, $u^i \in U(x^i)$ and $x^{i+1} \in Post(x^i, u^i)$.

Complex dynamical systems may motivate creating an abstraction of their model. Ideally, finding a control strategy for the abstraction would be simpler than for the original model. However, to control the original model with the controller of the abstraction, the systems must satisfy a formal behavioral relationship such as simulation or bisimulation. In the case of control systems with disturbances, we are interested in alternating simulation relations, defined in Tabuada (2009).

Definition 2. (Alternating simulation). Consider two systems S_a and S_b. A map $H : X_b \to X_a$ is an alternating simulation relation from S_a to S_b if it holds:

- $\forall x_{a0} \in X_{a0},\ \exists x_{b0} \in X_{b0} \mid x_{a0} = H(x_{b0})$;
- $\forall x_a = H(x_b),\ \forall u_a \in U_a(x_a),\ \exists u_b \in U_b(x_b)$ such that $\forall x_b' \in Post_b(x_b, u_b),\ H(x_b') \in Post_a(x_a, u_a)$.

We say that S_b alternatingly simulates the abstraction S_a and denote it as $S_a \preceq_{\mathcal{AS}} S_b$.

The second condition means that all the inputs of abstraction S_a have an equivalent in S_b such that all transitions in S_b are matched by a transition in the abstraction.

3. PROBLEM FORMULATION

We consider the system $S = (X, X_0, U, \longrightarrow)$ corresponding to a sampled version (with a constant sampling period $\tau \in \mathbb{R}^+$) of (1) where $X = \mathbb{R}^n$, $X_0 = [\underline{x}, \overline{x})$ is a half-closed interval ($x \in [\underline{x}, \overline{x}) \Leftrightarrow \overline{x} > x \geq \underline{x}$), $U = [\underline{u}, \overline{u}] \subset \mathbb{R}^p$ and $x \xrightarrow{u} x'$ if $\exists \mathbf{w} : [0, \tau] \to [\underline{w}, \overline{w}] \mid x' = \Phi(\tau, x, u, \mathbf{w})$. Our control objective is to meet the safety specification of maintaining the state of S in the interval $[\underline{x}, \overline{x})$.

In addition to the safety specification that may allow several values of the control input, we want to optimize a performance criterion given for a trajectory $(x^0, u^0, x^1, u^1, \dots)$ of the controlled system S by $\sum_{i=0}^{\infty} \lambda^i g(x^i, u^i)$, where $g(x, u)$ is the cost of choosing input u when the state of S is x and $\lambda \in (0, 1)$ is a discount factor to reduce the influence of the steps further in the future.

In what follows, we present two approaches based on abstractions to obtain such controllers of S. In Section 4, we use a centralized approach where we create an abstraction of the whole system S, while a compositional approach is considered in Section 5.

4. ABSTRACTION BASED CONTROL SYNTHESIS

4.1 Symbolic abstraction

We want to create a finite abstraction S_a of the sampled system S. To take advantage of the cooperativeness of our system (Definition 1), the set of initial states is chosen as a uniform partition $X_{a0} = \mathcal{P}^0$ of $[\underline{x}, \overline{x})$ into smaller identical half-closed intervals. For an element $s \in \mathcal{P}^0$, we denote as $\underline{s}$ and $\overline{s}$ its lower and upper bounds, respectively: $s = [\underline{s}, \overline{s}) \subseteq \mathbb{R}^n$. If we want $\alpha \in \mathbb{N}$ intervals per dimension in the partition, $\mathcal{P}^0$ can be expressed as follows:

$$\mathcal{P}^0 = \left\{ \left[\underline{s}, \underline{s} + \frac{\overline{x} - \underline{x}}{\alpha} \right) \mid \underline{s} \in \left(\underline{x} + \frac{\overline{x} - \underline{x}}{\alpha} * \mathbb{Z}^n \right) \cap [\underline{x}, \overline{x}) \right\},$$

where $*$ denotes the componentwise multiplication of vectors. The set of states of S_a is taken as $X_a = \mathcal{P}^0 \cup \{Out\}$ with $Out = \mathbb{R}^n \backslash [\underline{x}, \overline{x})$ such that X_a is a partition of $\mathbb{R}^n$. S_a is called a symbolic abstraction because each element $s \in \mathcal{P}$ can be seen as a symbol for all the states $x \in s$ of the original model S. To obtain a finite-transition system, we first need a finite input set. Similarly to the lower bounds $\underline{s}$ in $\mathcal{P}^0$, we discretize $U = [\underline{u}, \overline{u}]$ regularly into $\beta \geq 2$ values per dimension, including the lower and upper bounds:

$$U_a = \left(\underline{u} + \frac{\overline{u} - \underline{u}}{\beta - 1} * \mathbb{Z}^p \right) \cap U, \tag{2}$$

Then, we use the fact that (1) is cooperative to compute an over-approximation of the reachable set $Post([\underline{s}, \overline{s}), u)$: for all $x \in s = [\underline{s}, \overline{s})$, $\mathbf{w} : [0, \tau] \to [\underline{w}, \overline{w}]$, Definition 1 gives

$$\Phi(\tau, x, u, \mathbf{w}) \in [\Phi(\tau, \underline{s}, u, \underline{w}), \Phi(\tau, \overline{s}, u, \overline{w})]. \tag{3}$$

Hence, the successors of a symbol $s \in \mathcal{P}^0$ are those intersecting this over-approximation interval: $s \xrightarrow[a]{u} s'$ if $s' \cap [\Phi(\tau, \underline{s}, u, \underline{w}), \Phi(\tau, \overline{s}, u, \overline{w})] \neq \emptyset$. This method was presented in Moor and Raisch (2002) for the case of systems without disturbances. For simplicity and to ensure the alternating simulation, we consider that all possible transitions exist from symbol Out: $\forall u \in U_a,\ \forall s' \in \mathcal{P},\ Out \xrightarrow[a]{u} s'$. This choice has no consequence in what

follows since we are interested in the invariance of the interval $[\underline{x}, \overline{x})$ and these transitions will soon be discarded.

Proposition 3. The symbolic model S_a is alternatingly simulated by the original system S: $S_a \preceq_{\mathcal{AS}} S$

Proof. Consider $s = H(x) \Leftrightarrow x \in s$ as the candidate alternating simulation relation. The first condition of Definition 2 is immediately satisfied. For the second condition, let $s = [\underline{s}, \overline{s}) \in \mathcal{P}^0$, $x \in s$, $u \in U_a \subseteq U$ and $x' \in Post(x, u)$. From the definition of the transitions of S, $Post(x, u) \subseteq [\Phi(\tau, \underline{s}, u, \underline{w}), \Phi(\tau, \overline{s}, u, \overline{w})]$ which means that the symbol $s' = H(x')$ is such that $s' \in Post_a(s, u)$ and $x' \in s'$. Lastly, $\forall u \in U_a$, $Post_a(Out, u) = \mathcal{P}$, therefore any transition in S from $x \in Out$ can be matched by a transition in S_a. □

We can note that the symbolic model S_a described above is a finite-state and finite-transition abstraction of the initial system S. In addition, for a pair (s, u), checking the existing outgoing transitions $s \xrightarrow[a]{u} s'$ only requires to compute two successors in S (the bounds of s) and intersect the obtained over-approximation interval with the finite partition $\mathcal{P}$. This symbolic model can thus be built with a finite number of operations.

4.2 Receding horizon control

Safety We now aim to synthesize controllers of S that meet the specification of invariance of the interval $[\underline{x}, \overline{x})$. The corresponding safety specification for the abstraction S_a is the set $\mathcal{P}^0$. The safety game on S_a can be solved by introducing the operator $F_{\mathcal{P}^0} : 2^{\mathcal{P}} \to 2^{\mathcal{P}}$ such that:

$$F_{\mathcal{P}^0}(Z) = \{s \in Z \cap \mathcal{P}^0 \mid \exists u \in U_a,\ Post_a(s, u) \subseteq Z\}.$$

The set $F_{\mathcal{P}^0}(Z)$ contains all symbols $s \in Z \cap \mathcal{P}^0$ whose successors stay in Z for some $u \in U_a$. Note that $Post_a(s, u) \neq \emptyset$ since for all s, $U_a(s) = U_a$. Then the maximal fixed-point $Z_a = \lim_{i \to \infty} F^i_{\mathcal{P}^0}(\mathcal{P}^0)$ of $F_{\mathcal{P}^0}$ is computable in a finite number of steps and allows the definition of a non-deterministic controller $C_a : Z_a \to 2^{U_a}$ solving the safety game for S_a if $Z_a \neq \emptyset$ (Tabuada, 2009):

$$C_a(s) = \{u \in U_a \mid Post_a(s, u) \subseteq Z_a\}. \tag{4}$$

Performance optimization Then, we use a dynamic programming algorithm (Bertsekas, 1995) to minimize the cost of system S_a controlled with C_a over a finite horizon of N sampling periods. For a known initial state s^0, this cost $J_0(s^0)$ is computed iteratively following the principle of optimality (Bellman, 1957) for all k from N to 0:

$$J_k(s) = \min_{u \in C_a(s)} \left(g_a(s, u) + \lambda \max_{s' \in Post_a(s,u)} J_{k+1}(s') \right), \tag{5}$$

where $J_{N+1}(s) = 0$ for all $s \in \mathcal{P}^0$ and the cost function g_a is defined using the cost g on S from Section 3:

$$g_a(s, u) = \max_{x \in s} g(x, u). \tag{6}$$

At each iteration of (5), we minimize over safe inputs $u \in C_a(s)$ the sum of the cost of the current step and the worst case additive cost of all the following steps.

We can then apply a receding horizon control scheme

$$C^*_a(s) = \arg\min_{u \in C_a(s)} \left(g_a(s, u) + \lambda \max_{s' \in Post_a(s,u)} J_1(s') \right) \tag{7}$$

where at each sampling period we measure the current symbol s and only apply the first element of the control policy provided by (5). This approach is the basis of model predictive control (Rawlings and Mayne, 2009), with the difference that all the computations of (5) and (7) can be done offline for our finite transition system S_a. With the alternating simulation in Proposition 3, we can obtain a controller $C^X_a : [\underline{x}, \overline{x}) \to U$ of the sampled system S:

$$\forall s \in Z_a,\ \forall x \in s,\ C^X_a(x) = C^*_a(s) \in C_a(s). \tag{8}$$

4.3 Safety and performance guarantee

In this section, we show that the trajectories of S controlled with the receding horizon controller (8) satisfy the safety specification and we provide an explicit bound on their costs. We consider the following intermediate result.

Lemma 4. Let $M = \max_{s \in Z_a} J_N(s) = \max_{s \in Z_a} \min_{u \in C_a(s)} g_a(s, u)$. Then $J_0(s) \leq J_1(s) + \lambda^N M$ for all $s \in Z_a$.

Proof. This is proved by induction. For the initial step, we consider (5) with $k = N - 1$, the input $u \in C_a(s)$ satisfying $J_N(s) = g_a(s, u)$ and the definition of M:

$$J_{N-1}(s) \leq J_N(s) + \lambda \max_{s' \in Post_a(s,u)} J_N(s') \leq J_N(s) + \lambda M.$$

Assume now that $J_k(s) \leq J_{k+1}(s) + \lambda^{N-k} M$, then:

$$\begin{aligned} J_{k-1}(s) &= \min_{u \in C_a(s)} \left(g_a(s, u) + \lambda \max_{s' \in Post_a(s,u)} (J_k(s')) \right) \\ &\leq \min_{u \in C_a(s)} \left(g_a(s, u) + \lambda \max_{s' \in Post_a(s,u)} (J_{k+1}(s')) \right) \\ &\quad + \lambda^{N-k+1} M \\ &\leq J_k(s) + \lambda^{N-k+1} M. \end{aligned}$$

With $k = 1$, we obtain the result from Lemma 4. □

An upper bound on the performance criterion of S is then obtained when using the receding horizon controller C^X_a.

Theorem 5. Let $(x^0, u^0, x^1, u^1, \dots)$ be a trajectory of S controlled with C^X_a in (8), then $\forall k \in \mathbb{N}$, $x^k \in [\underline{x}, \overline{x})$. Moreover, let $s^0, s^1, \dots \in \mathcal{P}^0$ such that for all $k \in \mathbb{N}$, $x^k \in s^k$. Then, for all $k \in \mathbb{N}$,

$$\sum_{j=0}^{+\infty} \lambda^j g(x^{k+j}, u^{k+j}) \leq J_0(s^k) + \frac{\lambda^{N+1}}{1 - \lambda} M.$$

Proof. We know from (4) that C_a renders S_a invariant in the fixed point Z_a. With the alternating simulation from Proposition 3 and the definition of C^X_a in (8), if x^0 is initialized in a symbol $s^0 \in Z_a$, then the state of S controlled with C^X_a remains in $\{x \in \mathbb{R}^n \mid \exists s \in Z_a,\ x \in s\} \subseteq [\underline{x}, \overline{x})$. For the second part of the proposition, let $J(s) = J_0(s) + \frac{\lambda^{N+1}}{1-\lambda} M$. We start from the definition of $J_0(s^k)$ in (5) with $u^k = C^*_a(s^k)$ as in (7):

$$\begin{aligned} J(s^k) &= g_a(s^k, u^k) + \lambda \max_{s' \in Post_a(s^k, u^k)} (J_1(s')) + \frac{\lambda^{N+1}}{1 - \lambda} M \\ &\geq g_a(s^k, u^k) + \lambda J_1(s^{k+1}) + \frac{\lambda^{N+1}}{1 - \lambda} M \\ &\geq g_a(s^k, u^k) + \lambda \left(J_0(s^{k+1}) - \lambda^N M + \frac{\lambda^N}{1 - \lambda} M \right) \\ &\geq g(x^k, u^k) + \lambda J(s^{k+1}) \end{aligned}$$

The first inequality is obtained for a particular value $s' = s^{k+1}$ of the possible successors, the second comes

from Lemma 4 and the third from the definition (6) of g_a. Thus, if the inequality obtained above is applied to all the following states of the trajectory, we have for any k:

$$\begin{aligned} J(s^k) \geq & g(x^k, u^k) + \lambda J(s^{k+1}) \\ \geq & g(x^k, u^k) + \lambda g(x^{k+1}, u^{k+1}) + \lambda^2 J(s^{k+2}) \\ \geq & \cdots \end{aligned}$$

Expanding these inequalities to all states of the trajectory leads to the results from Theorem 5. □

Note that the constant part $\frac{\lambda^{N+1}}{1-\lambda} M$ of the upper bound in Theorem 5 goes to zero when the size N of the horizon used in the dynamic programming grows.

5. COMPOSITIONAL APPROACH

It is well known that scalability is one of the main limitations of the symbolic method presented in Section 4 due to the exponential complexity in the dimension n of the system. The idea presented in this section is to reduce the computational burden at the cost of lower precision: we decompose the system S into subsystems by considering only a subset of the state and control input components.

5.1 Subsystems

Let m be the number of subsystems, $(I_1, \ldots, I_m)$ a partition of $\{1, \ldots, n\}$ and $(J_1, \ldots, J_m)$ a partition of $\{1, \ldots, p\}$. For subsystem i, x_{I_i} and u_{J_i} are the vectors of observable states and controllable inputs, respectively. The remaining state and input components, denoted as x_{K_i} and u_{L_i} with $K_i = \{1, \ldots, n\} \backslash I_i$ and $L_i = \{1, \ldots, p\} \backslash J_i$, are considered as disturbances. For a set of indices I and a function, set or variable V, V_I represents the projection of V on the dimensions of indices in I. Similarly to an assume-guarantee reasoning (Alur and Henzinger, 1999), we assume that the other subsystems ensure the safety specification for the unobservable states: $x_{K_i} \in [\underline{x}_{K_i}, \overline{x}_{K_i})$. The symbolic abstraction corresponding to subsystem i is the finite automaton $S_i = (X_i, X_{i0}, U_i, \underset{i}{\longrightarrow})$ where $X_{i0} = \mathcal{P}^0_{I_i}$ and $U_i = U_{a,J_i}$ are the projections of $\mathcal{P}^0$ and U_a on the dimensions I_i of $\mathbb{R}^n$ or J_i of $\mathbb{R}^p$. Let Out^i be such that $X_i = \mathcal{P}^0_{I_i} \cup \{Out^i\}$ is a partition of X_{I_i} (projection of the continuous state space X on the dimensions in I_i). Using the simplified notations $\underline{\varphi_i}(\underline{s}_{I_i}, u_{J_i}) = \Phi_{I_i}(\tau, (\underline{s}_{I_i}, \underline{x}_{K_i}), (u_{J_i}, \underline{u}_{L_i}), \underline{w})$ and $\overline{\varphi_i}(\overline{s}_{I_i}, u_{J_i}) = \Phi_{I_i}(\tau, (\overline{s}_{I_i}, \overline{x}_{K_i}), (u_{J_i}, \overline{u}_{L_i}), \overline{w})$, the transition relation is defined as follows for all $s_{I_i} \in X_{i0}$, $u_{J_i} \in U_i$ and $s'_{I_i} \in X_i$:

- $s_{I_i} \underset{i}{\overset{u_{J_i}}{\longrightarrow}} s'_{I_i} \Leftrightarrow s'_{I_i} \cap [\underline{\varphi_i}(\underline{s}_{I_i}, u_{J_i}), \overline{\varphi_i}(\overline{s}_{I_i}, u_{J_i})] \neq \emptyset$;
- $Out^i \underset{i}{\overset{u_{J_i}}{\longrightarrow}} s'_{I_i}$.

Since Φ_{I_i} denotes the projection of Φ on the dimensions in I_i, we can clearly see that we obtain a less precise over-approximation of the reachable set due to the loss of observability of x_{K_i} and u_{L_i}. The second part of the transition definition is similar to the one of S_a.

Using a cost function $g^i : X_i \times U_i \to \mathbb{R}^+$, we can apply the controller synthesis approach presented in Section 4.2 to subsystem S_i and obtain the maximal fixed point $Z_i \subseteq X_{i0} = \mathcal{P}^0_{I_i}$ and the following three controllers for all $s \in Z_i$:

$$C_i(s) = \{u \in U_i \mid Post_i(s, u) \subseteq Z_i\}, \tag{9a}$$

$$C^*_i(s) = \underset{u \in C_i(s)}{\arg\min} \left(g^i(s, u) + \lambda \max_{s' \in Post_i(s,u)} J^i_1(s') \right), \tag{9b}$$

$$C^X_i(x) = C^*_i(s) \in C_i(s), \ \forall x \in s, \tag{9c}$$

where C_i is the safety controller associated to the fixed point Z_i, C^*_i is the receding horizon controller for S_i obtained from (5) and C^X_i the corresponding receding horizon controller on the continuous state space X_{I_i}.

5.2 Composition

Let $S_c = (\mathcal{P}, \mathcal{P}^0, U_a, \underset{c}{\longrightarrow})$ correspond to the composition of all subsystems S_i, with a transition relation defined by, $\forall s, s' \in \mathcal{P}^0$, $\forall u \in U_a$:

- $s \underset{c}{\overset{u}{\longrightarrow}} s'$ if $\forall i \in \{1, \ldots, m\}$, $s_{I_i} \underset{i}{\overset{u_{J_i}}{\longrightarrow}} s'_{I_i}$,
- $s \underset{c}{\overset{u}{\longrightarrow}} Out$ if $\exists i \in \{1, \ldots, m\} \mid s_{I_i} \underset{i}{\overset{u_{J_i}}{\longrightarrow}} Out^i$,
- $Out \underset{c}{\overset{u}{\longrightarrow}} s'$ and $Out \underset{c}{\overset{u}{\longrightarrow}} Out$.

We can then prove the alternating simulation between S_c and S_a and, by transitivity of $\preceq_{\mathcal{AS}}$, between S_c and S.

Proposition 6. $S_c \preceq_{\mathcal{AS}} S_a$ and $S_c \preceq_{\mathcal{AS}} S$.

Proof. Consider the identity as the candidate alternating simulation relation. The first condition of Definition 2 is immediately satisfied. Let $s \in \mathcal{P}$, $u \in U_a$ and $s' \in Post_a(s, u)$. If $s, s' \in \mathcal{P}^0$, then for all $i \in \{1, \ldots, m\}$, $s'_{I_i} \cap [\Phi_{I_i}(\tau, \underline{s}, u, \underline{w}), \Phi_{I_i}(\tau, \overline{s}, u, \overline{w})] \neq \emptyset$. Definition 1 gives:

$$\begin{cases} \Phi_{I_i}(\tau, (\underline{s}_{I_i}, \underline{x}_{K_i}), (u_{J_i}, \underline{u}_{L_i}), \underline{w}) \leq \Phi_{I_i}(\tau, \underline{s}, u, \underline{w}) \\ \Phi_{I_i}(\tau, (\overline{s}_{I_i}, \overline{x}_{K_i}), (u_{J_i}, \overline{u}_{L_i}), \overline{w}) \geq \Phi_{I_i}(\tau, \overline{s}, u, \overline{w}) \end{cases} \tag{10}$$

which implies that $s'_{I_i} \in Post_i(s_{I_i}, u_{J_i})$ for all i and then $s' \in Post_c(s, u)$. If $s' = Out$, $Out \in Post_a(s, u)$ means that there exists $j \in \{1, \ldots, n\}$ such that $\Phi_j(\tau, \underline{s}, u, \underline{w}) < \underline{x}_j$ or $\Phi_j(\tau, \overline{s}, u, \overline{w}) \geq \overline{x}_j$. Let $i \in \{1, \ldots, m\}$ such that $j \in I_i$, then (10) gives $Out^i \in Post_i(s_{I_i}, u_{J_i})$ which implies $Out \in Post_c(s, u)$. If $s = Out$ then $s' \in Post_c(Out, u) = \mathcal{P}$. The second result is obtained by transitivity of the alternating simulation (Tabuada, 2009) using Proposition 3. □

Since the subsystems partition the sets of state and input indices, the fixed points or controllers can simply be composed with a Cartesian product: let $Z_c = Z_1 \times \cdots \times Z_m$ and for all $s \in Z_c$ and $x \in s$,

$$C_c(s) = C_1(s_{I_1}) \times \cdots \times C_m(s_{I_m}) \tag{11a}$$

$$C^*_c(s) = (C^*_1(s_{I_1}), \ldots, C^*_m(s_{I_m})) \tag{11b}$$

$$C^X_c(x) = (C^X_1(x_{I_1}), \ldots, C^X_m(x_{I_m})) \tag{11c}$$

To obtain a result similar to Theorem 5, we need to introduce the following assumption.

Assumption 7. $g_a(s, u) \leq \sum_{i=1}^m g^i(s_{I_i}, u_{J_i})$ $\forall s \in Z_c$, $u \in U_a$ and $M \leq \sum_{i=1}^m M^i$ with $M^i = \max_{s_i \in Z_i} \min_{u_i \in C_i(s_i)} g^i(s_i, u_i)$.

Theorem 8. Let $(x^0, u^0, x^1, u^1, \ldots)$ be a trajectory of S controlled with C^X_c from (11c), then $\forall k \in \mathbb{N}$, $x^k \in [\underline{x}, \overline{x})$. Moreover, let $s^0, s^1, \cdots \in \mathcal{P}^0$ such that for all $k \in \mathbb{N}$, $x^k \in s^k$. Then, under Assumption 7, for all $k \in \mathbb{N}$,

$$\sum_{j=0}^{+\infty} \lambda^j g(x^{k+j}, u^{k+j}) \leq \sum_{i=1}^{m} J_0^i(s_{I_i}^k) + \frac{\lambda^{N+1}}{1-\lambda} \sum_{i=1}^{m} M^i.$$

Proof. Let $s \in Z_c$ and $x \in s$. By construction, $Post_i(s_{I_i}, C_i^X(x_{I_i})) \subseteq Z_i$. Then by definition of S_c, Z_c and C_c^X, we have $Post_c(s, C_c^X(x)) \subseteq Z_c$. Let $x' \in Post(x, C_c^X(x))$ and $s' \in \mathcal{P}$ such that $x' \in s'$. The alternating simulation from Proposition 6 gives $s' \in Post_c(s, C_c^X(x)) \subseteq Z_c$ which implies that $x' \in \{x \in \mathbb{R}^n \mid \exists s \in Z_c,\ x \in s\} \subseteq [\underline{x}, \overline{x})$.

For the second result, for each subsystem S_i, Assumption 7 gives $J_0^i(s_{I_i}) \leq J_1^i(s_{I_i}) + \lambda^N M^i$ for all $s_{I_i} \in Z_i$ similarly to Lemma 4. Then, as in the proof of Theorem 5 we obtain

$$\sum_{j=0}^{+\infty} \lambda^j g^i(s_{I_i}^{k+j}, u_{J_i}^{k+j}) \leq J_0^i(s_{I_i}^k) + \frac{\lambda^{N+1}}{1-\lambda} M^i. \tag{12}$$

Taking the sum of (12) over all subsystems, we obtain the inequality in Theorem 8 using (6) and Assumption 7: for all $x \in s$, $g(x,u) \leq g_a(s,u) \leq \sum_{i=1}^m g^i(s_{I_i}, u_{J_i})$. □

From the first part of Theorem 8, we can deduce the following result.

Corollary 9. $Z_c \subseteq Z_a$.

Proof. Z_c is an invariant set for S_c and with the alternating simulation from Proposition 6, it is also an invariant set for S_a. We also know that Z_a in Section 4.2 is the maximal invariant set of S_a for safety specifications in $\mathcal{P}^0$. □

We can also show that the cost obtained in (5) for S_a is smaller than the sum of those for the subsystems S_i.

Proposition 10. Under Assumption 7, for all $s \in Z_c$ we have $J_0(s) \leq \sum_{i=1}^m J_0^i(s_{I_i})$.

Proof. Let the cost function $g^c(s,u) = \sum_{i=1}^m g^i(s_{I_i}, u_{J_i})$. Since two functions g^i and g^j with $j \neq i$ are independent, the *min* and *max* operators on g^c can be decomposed into looking for its extrema for each $i \in \{1, \ldots, m\}$. The dynamic programming (5) applied to S_c using g^c and the safety controller C_c from (11a) thus has for solution the functions $J_k^c(s) = \sum_{i=1}^m J_k^i(s_{I_i})$ for all $s \in Z_c$. Define G_k^c and u_k^c as

$$G_k^c(s,u) = g^c(s,u) + \lambda \max_{s' \in Post_c(s,u)} J_{k+1}^c(s'),$$
$$u_k^c = \arg\min_{u \in C_c(s)} G_k^c(s,u),$$

such that $J_k^c(s) = \min_{u \in C_c(s)} G_k^c(s,u) = G_k^c(s, u_k^c)$ and assume we have similar notations $G_k^a(s,u)$ and u_k^a for S_a. Since $Z_c \subseteq Z_a$ and J_c^k is not defined on $Z_a \backslash Z_c$, we only focus on $s \in Z_c$ and prove the inequality by induction. The initial inequality $J_N(s) \leq J_N^c(s)$ is a consequence of the first part of Assumption 7. Next, assume that for all $s \in Z_c$, we have $J_{k+1}(s) \leq J_{k+1}^c(s)$. Then we have:

$$\begin{aligned} J_k(s) &= G_k^a(s, u_k^a) \leq G_k^a(s, u_k^c) \\ &\leq g^c(s, u_k^c) + \lambda \max_{s' \in Post_a(s, u_k^c)} J_{k+1}(s') \\ &\leq g^c(s, u_k^c) + \lambda \max_{s' \in Post_c(s, u_k^c)} J_{k+1}(s') \\ &\leq g^c(s, u_k^c) + \lambda \max_{s' \in Post_c(s, u_k^c)} J_{k+1}^c(s') = J_k^c(s). \end{aligned}$$

The four inequalities are obtained using, in this order, the definition of u_k^a, Assumption 7, the alternating simulation in Proposition 6 ($Post_a(s,u) \subseteq Post_c(s,u)$) and the induction hypothesis. □

Combining Proposition 10 with Assumption 7, we can see that, as expected, the performance guarantees from Theorem 5 are smaller than those from Theorem 8.

6. TEMPERATURE REGULATION IN BUILDINGS

System In this section, we illustrate the results of this paper on the temperature regulation in a flat equipped with *UnderFloor Air Distribution*, an alternative solution to traditional ceiling ventilation in buildings (Bauman and Daly, 2003) where the air is cooled in an underfloor plenum before being sent into each room. The temperature in a room is assumed to be uniform and the model of its variations is derived from the energy and mass conservation equations in this room. For a n-room building, the nonlinear dynamics of the system can thus be described by

$$\dot{T} = f(T, u, w, \delta), \tag{13}$$

where the n-dimensional vector field f depends on the temperature $T \in \mathbb{R}^n$, the control input $u \in [0,1]^n$ corresponds to the ventilation in each room, the exogenous inputs $w \in \mathbb{R}^3$ contains uncontrolled temperatures (underfloor, ceiling and outside) and the binary disturbance $\delta \in \{0,1\}^q$ represents the discrete state of heat sources in the rooms and the opening of doors. A detailed description of the system and the hypotheses to obtain (13) is given in Witrant et al. (2010) and Meyer et al. (2013), where we also prove that the model is cooperative as in Definition 1.

Abstraction The methods in Section 4 have been validated in Meyer et al. (2015) on an experimental 4-room small-scale building. To facilitate visualization, in this paper we consider the model (13) for a 2-room flat. We define the symbolic model S_a as in Section 4.1 with a partition $\mathcal{P}^0$ of the state interval $[\underline{T}, \overline{T}) \subset \mathbb{R}^2$ into 10×10 symbols (half-closed intervals) and a control set U_a obtained as in (2) from a discretization of $U = [0,1]^2$ with $\beta = 5$ values per dimension. The sampling period τ has to be chosen as a tradeoff between large values to avoid self loops for the optimization and small values to avoid large variations that might prevent finding a non-empty fixed-point.

Safety An illustration of the controller synthesis proposed in Section 4.2 on the symbolic abstraction S_a is depicted in Figure 1. In all three examples of this figure, we represent the partition $\mathcal{P}^0$ of the target interval as the red grid and the symbols colored in yellow are those in the fixed-point Z_a solving the safety specification. In the first graph of Figure 1, we want to keep the temperature of both rooms in an interval $[22, 24]$ and we can see that $Z_a = \mathcal{P}^0$, which means that for each symbol in the interval there exists a value of the ventilation keeping both temperatures in their intervals in any condition of the disturbances. This case can be linked to the notion of robust controlled invariant interval defined in Meyer et al. (2013). The second graph of Figure 1 corresponds to a similar partition but with the target interval for room 2 shifted to $[20, 22]$. In these conditions, we can see that the largest fixed-point Z_a for S_a does not cover the whole interval but is much larger than the maximal robust controlled invariant sub-interval for the continuous system (1). This is due to the fact that

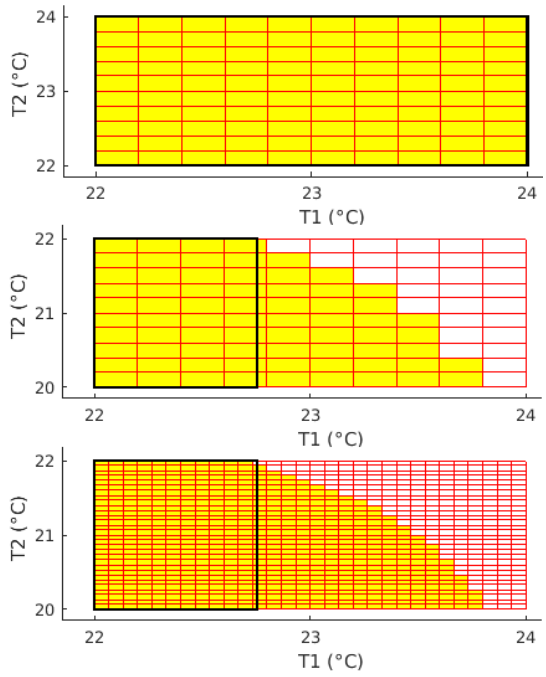

Fig. 1. Fixed-points Z_a (yellow) for S_a and largest robust controlled invariant sub-interval (black).

the symbolic approach allows non-rectangle invariants. In the same conditions, the third graph of Figure 1 represents the fixed-point Z_a when the symbolic model S_a is created with a finer partition (30×30 symbols) of the interval. If we keep increasing the precision of the partition and reduce the sampling time accordingly, Z_a converges to the maximal robust controlled invariant subset of the interval and we can see that we already obtain a good approximation with 10×10 symbols. With the compositional approach from Section 5, the fixed-points Z_c obtained in the three conditions of Figure 1 are $Z_c = Z_a = \mathcal{P}^0$ in the first case and $Z_c = \emptyset$ in the others, which confirms that $Z_c \subseteq Z_a$.

Complexity On the other hand, the compositional approach compensates the loss of precision in its subsystems by a significant increase in computation efficiency. If we consider the model (13) for a n-room building with α symbols and β control values per dimension as in Section 4.1, the symbolic abstraction S_a can be obtained by computing $2(\alpha\beta)^n$ successors of the sampled system S, while the composed system S_c only needs $n*2\alpha\beta$. Thus we go from an exponential complexity in n and a polynomial one in α and β for S_a to a linear complexity in n, α and β for S_c. In the configuration presented below for the 2-room building, S_a and C were obtained after $26s$ while S_c and C_c only required $0.13s$ (on a 3GHz CPU). In a 4-room building, the centralized method (S_a, C) for the experimental implementation presented in Meyer et al. (2015) took a couple of days while the compositional method only needs $0.4s$ in the same conditions.

Performances The dynamic programming algorithm is run over a finite time window of size $N = 5$ and with a discount factor $\lambda = 0.5$. These values are chosen such that the constant part of the upper bound in Theorems 5 and 8 is small enough: $\lambda^{N+1}/(1-\lambda) \approx 3\%$. The cost function g at step k is defined as the combination of three criteria

Criterion	k	C_a^X	C_c^X
$\sum_{j=0}^{+\infty} \lambda^j g(x^{k+j}, u^{k+j})$	$k = 0$	0.2004	0.1227
Guaranteed upper bound(x^k)		0.2873	0.3216
$\sum_{j=0}^{+\infty} \lambda^j g(x^{k+j}, u^{k+j})$	$mean_{k\in\mathbb{N}}$	0.1790	0.1458
Guaranteed upper bound(x^k)		0.3158	0.3135

Table 1. Costs on the trajectories of Figure 2.

to be minimized: the norm $\|u^k\|$ of the control input, its variations $\|u^k - u^{k-1}\|$ requiring to introduce an extended state $z^k = (T^k, u^{k-1})$ (Bertsekas, 1995) and the distance $\|T^k - T^*\|$ between the state T^k and the center T^* of the interval. To have comparable influences, the three criteria are normalized and associated with a $1/3$ weight. Using the square of the 2-norm, the first part of Assumption 7 is satisfied with an equality. The second part of Assumption 7 is verified numerically: $M^1 = M^2 = M/2 = 0.33$.

To compare the results with both the centralized and the compositional approaches, we consider the conditions of the first graph of Figure 1 where both Z_a and Z_c are non-empty. We can first check that Proposition 10 is satisfied: over all symbols $s \in Z_a$, $J_0^1(s_1) + J_0^2(s_2) - J_0(s)$ varies between 0 and 0.92 with a mean value of 0.016, while the maximal value of either side of the inequality is 0.99. In Figure 2, we represent the temperature and ventilation of system (13) controlled with C_a^X from the centralized method in Section 4 (red dashed curve or upward triangles) and C_c^X from the compositional approach in Section 5 (blue plain curve or downward triangles). The simulations are run with sinusoidal exogenous inputs and the discrete disturbances are such that all possible combinations appear: the heat source in room 1 is on from 13 to 36 and from 61 to 84 minutes, in room 2 from 25 to 72 minutes and the door is open after 49 minutes (until the end). First, we can see that both controllers correctly maintain the state of the system in the prescribed bounds. For the second part of Theorems 5 and 8, we compute the cost $\sum_{j=0}^{+\infty} \lambda^j g(x^{k+j}, u^{k+j})$ of the trajectory from any sampling time k (discarding the last 10 having too short trajectories) and verify that it is smaller than the guaranteed upper bound provided in Theorems 5 and 8 corresponding to the same sampling time k. The value of both sides of these inequalities for the initial state x^0 of the trajectories of S respectively controlled with C_a^X and C_c^X are reported in the top of Table 1. We only look at the initial state since it is the only step where we know that the trajectories are in the same state. We can first see two expected results: the cost of the trajectories are smaller than their respective guaranteed upper bounds as in Theorems 5 and 8 and the guaranteed upper bound for the compositional method is larger than the centralized one as in Proposition 10. There is however a surprising result that the actual performance from the initial state are better for the compositional method. This is confirmed when computing the average value of the performance criterion from any point of the trajectories, while the average on the corresponding guaranteed upper bounds are comparable for both methods (bottom of Table 1). This could be explained by the fact that C_a^X and C_c^X are obtained with worst-case considerations on the disturbances. Since more disturbances are involved in the compositional method (unobservable states and inputs), C_c^X naturally is more conservative, which gave better performances in this particular simulation.

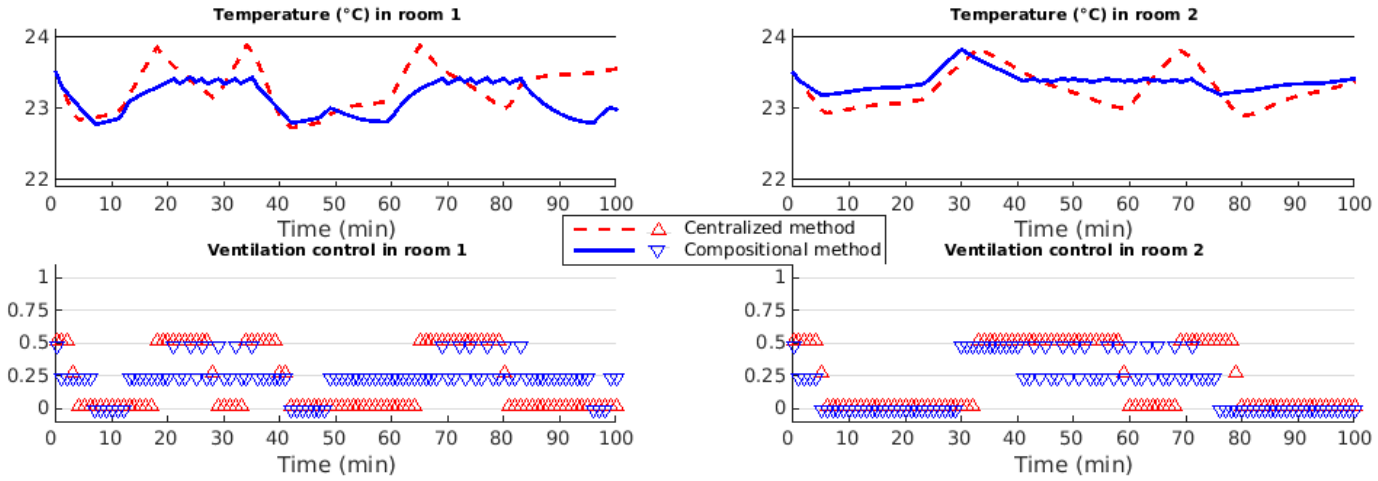

Fig. 2. $2D$ system (13) controlled with the controllers from the centralized (red) and compositional (blue) methods.

7. CONCLUSION

We presented two methods to obtain a symbolic abstraction, in the sense of alternating simulation, of a class of non-linear systems subject to disturbances and satisfying the cooperativeness property. The first one is a centralized approach where an abstraction of the whole system is created, while a compositional approach is considered in the second method to reduce the complexity of the problem at the cost of the precision of the abstraction. These symbolic abstractions are then used to synthesize a controller ensuring a safety specification on the original system and minimizing some cost criterion. For both approaches, we provide performance guarantees in the form of an upper bound for the total cost of the controlled original system on any infinite time horizon. We also show that the guaranteed performances for the centralized method are, as expected, better than those for the compositional approach. Finally, these theoretical results are illustrated on the temperature regulation in a 2-room building. In particular, we can observe on these simulations the large reduction in computation time with the compositional method for a relatively small or no loss of performance compared to the centralized approach. This compositional approach thus provides the opportunity to apply symbolic methods in a real-time implementation and to systems of larger dimensions that could not be handled otherwise.

REFERENCES

Alur, R. and Henzinger, T.A. (1999). Reactive modules. *Formal Methods in System Design*, 15(1), 7–48.

Alur, R., Henzinger, T.A., Lafferriere, G., and Pappas, G.J. (2000). Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(7), 971–984.

Angeli, D. and Sontag, E.D. (2003). Monotone control systems. *IEEE Transactions on Automatic Control*, 48(10), 1684–1698.

Bauman, F.S. and Daly, A. (2003). *Underfloor air distribution (UFAD) design guide*. ASHRAE.

Belgacem, I. and Gouzé, J.L. (2013). Global stability of enzymatic chains of full reversible Michaelis-Menten reactions. *Acta biotheoretica*, 61(3), 425–436.

Bellman, R. (1957). *Dynamic Programming*. Princeton University Press.

Bertsekas, D.P. (1995). *Dynamic programming and optimal control*, volume 1. Athena Scientific Belmont, MA.

Coogan, S. and Arcak, M. (2015). Scalable finite abstraction of mixed monotone systems. In *Hybrid Systems: Computation and Control*, 58–67.

Ding, X., Lazar, M., and Belta, C. (2014). LTL receding horizon control for finite deterministic systems. *Automatica*, 50(2), 399–408.

Meyer, P.J., Girard, A., and Witrant, E. (2013). Controllability and invariance of monotone systems for robust ventilation automation in buildings. In *Proceedings of the* 52^{nd} *IEEE Conference on Decision and Control*, 1289–1294.

Meyer, P.J., Girard, A., and Witrant, E. (2015). Symbolic control of monotone systems, application to ventilation regulation in buildings. In *Hybrid Systems: Computation and Control*, 281–282.

Moor, T. and Raisch, J. (2002). Abstraction based supervisory controller synthesis for high order monotone continuous systems. In *Modelling, Analysis, and Design of Hybrid Systems*, 247–265. Springer.

Pola, G., Girard, A., and Tabuada, P. (2008). Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10), 2508–2516.

Rawlings, J.B. and Mayne, D.Q. (2009). *Model predictive control: Theory and design*. Nob Hill Pub.

Reißig, G. (2009). Computation of discrete abstractions of arbitrary memory span for nonlinear sampled systems. In *Hybrid Systems: Computation and Control*, 306–320.

Skogestad, S. and Postlethwaite, I. (2005). *Multivariable feedback control: analysis and design*. Wiley, 2^{nd} edition.

Smith, H.L. (1995). *Monotone dynamical systems: an introduction to the theory of competitive and cooperative systems*, volume 41. American Mathematical Soc.

Sontag, E.D. (2007). Monotone and near-monotone biochemical networks. *Systems and Synthetic Biology*, 1(2), 59–87.

Tabuada, P. (2009). *Verification and control of hybrid systems: a symbolic approach*. Springer.

Witrant, E., Di Marco, P., Park, P., and Briat, C. (2010). Limitations and performances of robust control over WSN: UFAD control in intelligent buildings. *IMA Journal of Mathematical Control and Information*, 27(4), 527–543.